UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,986	05/22/2001	Hezi Friedman	P04949 (NATI15-04949)	7516

7590 03/24/2005

William A. Munck
Novakov Davis & Munck, P.C.
13155 Noel Road, Suite 900
Dallas, TX 75240

EXAMINER	
AKPATI, ODAICHE T	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

HL

Office Action Summary	Application No.	Applicant(s)	
	09/862,986	FRIEDMAN ET AL.	
	Examiner	Art Unit	
	Tracey Akpati	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 17 March 2003 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2 are rejected under 35 U.S.C. 102(e) as being anticipated by Rawlins (6216183).

With respect to Claim 1, the limitation of "an apparatus for providing a secure universal serial bus (USB) comprising a secure channel for transferring data" is met on Fig. 1 and on column 2, lines 41-50. USB represents the secure universal serial bus because the USB host controller polls the USB keyboard (USB device 32a on Fig. 1) for information and places it in a data buffer and later on a system memory of a host computer. The host controller prevents access during normal computer operation to these two storage locations hence preventing unauthorized access to data and/or information entered via the USB keyboard. Therefore the USB is secure.

With respect to Claim 2, the limitation of "wherein said apparatus comprises a secure USB domain device coupled to an external host computer" is met on Fig. 1 and on column 3, lines 8-18, 48-50. The computer system represents the external host computer.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rawlins (6216183).

With respect to Claim 3, the limitation of "a USB memory device that is not accessible by said host computer" is met on column 3, lines 12-18 and on column 1, lines 21-30; and "a USB processor that is not accessible by said host computer" is met on column 3, lines 3-11; and "a USB host controller that is not accessible by said host computer" is met on column 3, lines 26-40, and column 2, lines 20-31; and "an internal USB bus that couples said USB memory ,device, said USB processor, and said USB host controller" is met on Fig. 1. The system memory represents the USB memory device and the processor represents the USB processor. The system memory stores sensitive information that is not accessible during normal operation of the computer system. It is also inaccessible to an unauthorized user. The processor and USB host controller, because they support and work in conjunction with the system memory to achieve this goal is also inaccessible during this same period.

It would have been obvious to one of ordinary skill in the art to have the USB memory device, processor and host controller inaccessible to the host computer so as to prevent unauthorized access to data by a malicious computer user.

With respect to Claim 4, the limitation of "a USB node coupled to said USB bus, said USB node capable of being coupled to a USB tree" is met on Fig. 1. The USB device represents the USB node.

Claims 5, 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rawlins (6216183) in view of Flannery (5799196).

With respect to Claim 5, all the limitation is met by Rawlins except for the following limitation.

The limitation of "wherein said apparatus comprises a secure USB domain device embedded within a host computer" is met by Flannery on column 2, lines 12-14, 18-22.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Flannery within the system of Rawlins because an embedded USB domain device creates a hierarchical topology that enhances the scalability of the computer system. Hence more hosts and/or peripheral devices can be connected to the root host to achieve greater efficiency.

With respect to Claim 6, Rawlins meets the limitation of "a USB memory device that is not accessible by said host computer" on column 3, lines 12-18, column 1, lines 21-30; and "a USB processor that is not accessible by said host computer" on column 3, lines 3-11; and "a USB host controller that is not accessible by said host computer" is met on column 3, lines 26-40; and "an internal USB bus that couples said USB memory device, said USB processor, and said USB host controller" on Fig. 1.

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rawlins (6216183) in view of Flannery (5799196) in further view of Ben-Dor et al (US2002/0141418 A1).

With respect to Claim 7, all the limitation is met by the combination of Rawlins and Flannery except for the following limitation.

The limitation of "virtual conduit interface coupled to said secure USB domain device and coupled to at least one non-USB device, said virtual conduit interface capable of providing a secure USB channel for transferring information to said at least one non-USB device" is met by Ben-Dor et al on paragraph 73. The virtual USB host controller represents the virtual conduit interface (VIC). Tunneling is a secure form of communication between two parties and hence a secure channel is created for transferring information to a non-USB hardware.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Ben-Dor et al within the combination of Rawlins and Flannery so as to allow for the USB controller to interface with non-USB hardware.

Claims 8-11, 13-15, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5799196) in view of Rawlins (6216183).

With respect to Claim 8, Flannery meets the limitation of "an apparatus for providing a secure universal serial bus (USB) capable of transferring information over a secure channel to and from a device coupled to a host computer, wherein said host computer is coupled to other host computers in a data network; and at least one host computer capable of supporting USB

input/output devices, said at least one host computer comprising a USB bus, USB client software, and USB System software" is met on column 2, lines 5-8, 12-15, 18-22. USB software on column 2, lines 14-20 represents the USB client software and USB system software. Flannery however does not meet the following limitation.

The limitation of "a secure USB domain device capable of one of blocking outgoing data flows of confidential information, forwarding outgoing data flows of encrypted confidential information, and forwarding outgoing data flows of non-confidential information" is met by Rawlins on column 2, lines 62-67 and on column 3, lines 1-18. It is obvious to encrypt the confidential information so as to prevent an intruder from deciphering the confidential information.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Rawlins within the system of Flannery because a secure USB domain device capable of blocking outgoing flows of confidential data will prevent secret information leaking to an outsider who may potentially sabotage the confidentiality of that information.

With respect to Claim 9, Flannery meets all the limitation except for the following limitation.

The limitation of "a plurality of USB devices; and a first set of data channels for exchanging data with each of said plurality of USB devices; and a second set of data channels for exchanging data between said secure USB domain device and said at least one host computer" is

met by Rawlins in Fig. 1. The USB represents the first set of data channels while the peripheral and CPU buses represent the second set of data channels.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Rawlins within the system of Flannery because a secure USB domain device capable of blocking outgoing flows of confidential data will prevent secret information from leaking to an outsider who may potentially sabotage the confidentiality of that information.

With respect to Claim 10, Flannery meets the limitation of "wherein said secure USB domain device is embedded within said at least one host computer" on column 2, lines 12-14.

With respect to Claims 11 and 14, Flannery meets all the limitation except for the following limitation.

Rawlins meets the limitation of "a USB bus" in Fig. 1; and "a memory coupled to said USB bus capable of storing each data packet sent from, or received by, said secure USB domain device, said memory containing a set of buffers, each of said buffers comprises data associated with said Host or to said device" in Fig. 1 and on column 3, lines 40-47 (the data buffer of the USB host controller represents the memory); and "circuitry coupled to said USB bus, said circuitry capable of forwarding commands and requests for information received in said secure USB domain device to corresponding devices" is met in Fig. 1(USB host controller provides such circuitry); and "a processor coupled to said USB bus, said processor capable of one of classifying data packets, controlling forwarding operations, and controlling encryption

operations" is met on column 3, lines 31-40 and on column 4, lines 14-23 (the control unit of the host controller represents the processor); and "a USB host controller coupled to said USB bus, said USB host controller capable of managing data flow between said at least one host computer and a plurality of USB devices" is met on column 2, lines 46-55 and on column 3, lines 26-31.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Rawlins within the system of Flannery because a secure USB device capable of screening forwarded flows of confidential data will prevent secret information from leaking to an attacker who may potentially sabotage the confidentiality of that information.

With respect to Claim 13, Flannery meets all the limitation except for the following limitation.

Rawlins meets the limitation of "wherein said secure USB domain device is coupled to said at least one external host computer" on Fig 1 and on column 3, lines 8-18, 48-50.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Rawlins within the system of Flannery because a secure USB domain device capable of blocking outgoing flows of confidential data will prevent secret information leaking to an outsider who may potentially sabotage the confidentiality of that information.

With respect to Claim 15, its limitation is similar to Claim 8 limitation. The difference is that Claim 15 is the method claim of Claim 8, an apparatus claim. Hence its rejection can be found therein.

With respect to Claim 19, Flannery meets all the limitation except for the following limitation.

Rawlins meets the limitation of "wherein data flows from a first device to a second device directly through said secure USB domain device without utilizing resources of said host computer" on column 8, lines 25-32.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Rawlins within the system of Flannery because a secure USB domain device will screen its outgoing data flows and prevent access to the data from an unauthorized user. This enhances the integrity of the USB device.

Claims 12 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5799196) in view of Rawlins (6216183) in further view of Ben-Dor et al (US2002/0141418 A1).

With respect to Claim 12, all the limitation is met by the combination of Flannery and Rawlins except for the following limitation.

The limitation of "wherein said apparatus further comprises a virtual conduit interface coupled to said secure USB domain device and coupled to at least one non-USB device, said virtual conduit interface capable of providing a secure USB channel for transferring information to said at least one non-USB device" is met by Ben-Dor et al on paragraph 73. The virtual USB controller represents the virtual conduit interface (VIC).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Ben-Dor et al within the combination of Flannery and Rawlins so as to allow for the USB controller to interface with non-USB hardware.

With respect to Claim 20, all the limitation is met by the combination of Flannery and Rawlins except for the following limitation.

The limitation of "coupling a virtual conduit interface to said secure USB domain device; coupling said virtual conduit interface to at least one non-USB device; and using said virtual conduit interface to provide a secure USB channel for transferring information to said at least one non-USB device" is met by Ben-Dor et al on paragraph 73.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Ben-Dor et al within the combination of Flannery and Rawlins so as to allow for the USB controller to interface with non-USB hardware.

Claims 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Flannery (5799196) in view of Rawlins (6216183) in further view of Lemay et al (US2002/0144115 A1).

With respect to Claim 16, Flannery meets all the limitation except the following limitation.

Rawlins meets the limitation of "storing each data packet received by said secure USB domain device in a memory containing a set of buffers, each of said buffers comprising data associated with one of: said at least one host computer, and said device coupled to

said at least one host computer" on column 3, lines 40-52; and "forwarding commands and requests for information received in said secure USB domain device to a corresponding device" on column 3, lines 62-67 and on column 4, lines 1-11; and "classifying each data packet sent from said device to said secure USB domain device to one of a first data type that requires no intervention, and a second data type that requires intervention according to a buffer association" on column 4, lines 14-23 (the non-secured data represents the first data type and the secured data represents the second data type); and "forwarding data packets of the first type that are originated at said device to said at least one host computer" is met on column 8, lines 25-32; and "blocking data packets of the second type that contain confidential information; forwarding data packets of the second type that contain encrypted confidential information; and forcing any exchange of data between said at least one host computer and said device to flow through said secure USB domain device" is partly met on column 3, lines 18-25 and on column 4, lines 14-24, 35-43. Rawlins however does not disclose encryption of the information. Lemay et al discloses this on paragraphs 58 and 59.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Lemay et al within the combination of Flannery and Rawlins so as to prevent the deciphering of confidential information by an intruder.

With respect to Claim 17, Flannery meets all the limitation except for the following limitation.

Rawlins meets the limitation of "interrogating a header of each data packet of the second type to reveal the type of information required from a device" on column 7, lines 44-53; and

"transferring said information in an encrypted form if the information is required at another host computer for further actions" partly on column 4, lines 14-24; and "blocking the data packet" is met on column 3, lines 18-25. Rawlins however does not meet the limitation above of transferring encrypted information. This is met by Lemay et al on paragraph 59.

Lemay et al meets further limitation of "receiving verification information from said host computer in an encrypted form" on paragraphs 58 and 59; and "decrypting said verification information" on paragraph 78; and "comparing said encrypted verification information with information received from said device; and providing said host computer with an indication verifying whether a match was detected" on paragraph 78.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Lemay et al within the combination of Flannery and Rawlins so as to prevent the deciphering of confidential information by an intruder.

With respect to Claim 18, Flannery meets all the limitation except for the following limitation.

Rawlins meets the limitation of "wherein secure information is transferred between said host computer and said secure USB domain device in a enciphered form, thereby establishing at least one secure data channel between said host computer and said secure USB domain device" on column 3, lines 49-58. Rawlins however does not disclose the limitation of transferring of information in enciphered form. Lemay discloses this on paragraph 58 and 59.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Lemay et al within the combination of Flannery and Rawlins so as to prevent the deciphering of confidential information by an intruder.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 571-272-3846. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

OTA